MATH 430 HW2

Qilin Ye

September 3, 2020

Problem 1. If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod{n}$ where $n = \gcd(n_1, n_2)$.

Proof. Suppose $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{c_2}$. Then it follows that

$$n_1 \mid a - b \text{ and } n_2 \mid a - c.$$

Since $\gcd(n_1, n_2) \mid n_1$ and $\gcd(n_1, n_2) \mid n_2$, we also have

$$\gcd(n_1, n_2) \mid a - b \text{ and } \gcd(n_1, n_2) \mid a - c.$$

If $\gcd(n_1, n_2)$ divides both $(a - b)$ and $(a - c)$, it also divides their difference, namely

$$\gcd(n_1, n_2) \mid (a - c) - (a - b) \implies \gcd(n_1, n_2) \mid b - c.$$

Therefore b and c have the same remainder when divided by $\gcd(n_1, n_2)$, i.e., $b \equiv c \pmod{\gcd(n_1, n_2)}$. □

Problem 2. Solve for x where $x^2 \equiv 35 \pmod{100}$. Hint: look for $\pmod{10}$.

Solution. Note that if $x^2 \equiv 35 \pmod{100}$ then $x^2 = 100k + 35$ for some integer k. Clearly the RHS is a multiple of 5. This implies $5 \mid x^2$, which further implies $5 \mid x$ since 5 is a prime. Also note that $2 \nmid 100k + 35$ which implies $2 \nmid x^2$ and therefore $2 \nmid x$. Any odd multiple of 5 has the form $10m + 5$, and their squares have the form

$$(10m + 5)^2 = 100m^2 + 100m + 25 = 100(m^2 + m) + 25$$
$$\implies x^2 \equiv 25 \pmod{100}$$

Therefore we see that, if x is an odd square, its square must $\equiv 25 \pmod{100}$. So $x^2 \equiv 35 \pmod{100}$ has no solution.

Problem 3. A certain integer between 1 and 1200 leaves remainders $1, 2, 6$ when divided by $9, 11, 13$ respectively. What is this integer?

Solution. We first find an integer a, a multiple of $11 \cdot 13$, that satisfies $a \equiv 1 \pmod{9}$. Then we find another integer b, a multiple of $9 \cdot 13$, that satisfies $b \equiv 2 \pmod{11}$. Lastly, we find another integer c, a multiple of $9 \cdot 11$, that satisfies $c \equiv 6 \pmod{13}$. In this way, since both a and b are multiples of 13, we have $a + b + c \equiv c \equiv 6 \pmod{13}$.

Similarly for $\pmod 9$ and $\pmod{11}$. R educing three congruence relations to two significantly lowers the amount of calculation required.

Since $11 \cdot 13 = 143 \equiv -1 \pmod 9$, we can set $a = -143$ so that $a \equiv -(-1) \equiv 1 \pmod 9$.

For b, since $9 \cdot 13 = 117 \equiv 7 \pmod{11}$, we have $5 \cdot 117 \equiv 5 \cdot 7 \equiv 2 \pmod{11}$. Therefore we may set $b = 5 \cdot 117 = 585$.

Lastly, since $11 \cdot 9 = 99 \equiv 8 \pmod{13}$, we have $4 \cdot 99 \equiv 4 \cdot 8 \equiv 6 \pmod{13}$. Therefore we may set $c = 4 \cdot 99 = 396$.

Adding a, b, c gives $-143 + 585 + 396 = 838$, our desired number. Since

$$838 - \operatorname{lcm}(9, 11, 13) < 1 < 838 < 1200 < 838 + \operatorname{lcm}(9, 11, 13),$$

we claim that 838 is the only integer that satisfies all three requirements between 1 and 1200.